REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

OFFRE DE FORMATION
L.M.D.

MASTER ACADEMIQUE

(Reconduction avec diminution du nombre de postes)

Etablissement	Faculté	Département
Université de Batna	**Faculté des Sciences**	**Informatique**

Domaine	Filière	Spécialité
Mathématiques et Informatique	**Informatique**	**Cryptographie et Sécurité**

Responsable de l'équipe du domaine de formation :
Prof. Noui Lemnouar

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

عرض تكوين

ل. م . د

ماستر أكاديمي

المؤسسة	الكلية	القسم
جامعة باتنة	كلية العلوم	قسم الإعلام الآلي

الميدان	الشعبة	التخصص
رياضيات و الأعلام الآلي	**الإعلام الآلي**	**علم التشفير**

مسؤول فرقة ميدان التكوين :
الأستاذ : النوي لمنور

SOMMAIRE

Page

I - Fiche d'identité du Master..... 4
1 - Localisation de la formation..... 5
2 - Coordonnateurs..... 5
3 - Partenaires extérieurs éventuels..... 5
4 - Contexte et objectifs de la formation..... 5
A - Organisation générale de la formation : position du projet..... 5
B - Conditions d'accès..... 6
C – Objectifs de la formation..... 6
D - Profils et compétences visées..... 6
E - Potentialités régionales et nationales d'employabilité..... 6
F - Passerelles vers les autres spécialités..... 7
G - Indicateurs de suivi du projet de formation..... 7
5 - Moyens humains disponibles..... 8
A – Capacité d'encadrement..... 8
B - Equipe d'encadrement de la formation..... 8
B-1 : Encadrement Interne..... 8
B-2 : Encadrement Externe..... 10
B- 3 : Synthèse globale des ressources humaines..... 10
B-4 : Personnel permanent de soutien..... 10
6 - Moyens matériels disponibles..... 11
A - Laboratoires Pédagogiques et Equipements..... 11
B- Terrains de stage et formations en entreprise..... 11
C - Laboratoires de recherche de soutien à la formation proposée..... 11
D - Projets de recherche de soutien à la formation propos..... 12
E - Documentation disponible..... 12
F - Espaces de travaux personnels et TIC..... 13
II - Fiche d'organisation semestrielle des enseignements..... 14
1- Semestre 1..... 15
2- Semestre 2..... 16
3- Semestre 3..... 17
4- Semestre 4..... 18
5- Récapitulatif global de la formation..... 18
III - Fiche d'organisation des unités d'enseignement..... 19
IV - Programme détaillé par matière..... 34
V – Accords / conventions..... 56
VI – Curriculum Vitae des coordonnateurs..... 59
VII - Avis et Visas des organes administratifs et consultatif..... 68
VIII - Visa de la Conférence Régionale..... 69

I – Fiche d'identité du Master

1 - Localisation de la formation :

Faculté (ou Institut) : Faculté des Sciences
Département : Informatique
Section : Informatique

2 – Coordonnateurs :

- Responsable de l'équipe du domaine de formation

Nom & prénom: Noui Lemnouar
Grade : Professeur
☎ : 0778166364 Fax : 033868964 E - mail : nouilem@yahoo.fr

- Responsable de l'équipe de la filière de formation

Nom & prénom: Bilami Azzedine
Grade: Professeur
☎ : Fax : E - mail : abilami@yahoo.fr

- Responsable de l'équipe de spécialité

Nom & prénom: Noui Lemnouar
Grade : Professeur
☎ : 0778166364 Fax : 033868964 E - mail : nouilem@yahoo.fr

3- Partenaires extérieurs *:

- autres établissements partenaires :

  Département de mathématiques

  Département d'électronique

- entreprises et autres partenaires socio économiques :

- Partenaires internationaux :

4 – Contexte et objectifs de la formation

A – Organisation générale de la formation : position du projet

Première année de Master
Deuxième année de Master

B – Conditions d'accès

Après étude du dossier par l'équipe de formation, ce master est accessible aux étudiants ayant :

- *Une licence académique d'informatique LMD,*
- *Une licence académique de Mathématiques LMD,*

(Priorité donnée au licence dont le programme est adéquat avec la formation proposée)

C - Objectifs de la formation

L'objectif du master proposé et de former des cadres à profil d'experts spécialisés dans les domaines de la cryptologie et de la sécurité informatique. Ses diplômés auront une solide formation théorique en mathématiques et en informatique, compétences qu'ils verront appliquées à des problèmes pratiques en cryptographie et sécurité dans les entreprises privés et publiques.

Plus précisément, ce master permettra aux étudiants de :

1) Acquérir les notions fondamentales :
   - En mathématiques (algèbre, arithmétique),
   - En informatique (algorithmique, théorie de la complexité, programmation orientée objet),

2) Maîtriser les outils spécifiques au traitement de l'information (codes correcteurs d'erreurs, cryptographie, algorithmique arithmétique, traitement de signal et de l'image, sécurité des réseaux, etc.).

3) Explorer et maître en œuvre les notions étudiées en vue de développer des cryptosystèmes pour la protection de l'information.

D – Profils et compétences visées

Notre spécialité vise à former des doctorants en informatique.

Les applications visées sont

Traitement et protection de l'information, tels que :

- Sécurité des réseaux (toutes entreprises)
- Sécurisation des transactions sur Internet (banques, services…)
- Télécommunications
- Cryptographie (carte à puces, secteur militaire).

E- Potentialités régionales et nationales d'employabilité

Dans tous les domaines : entreprises, enseignement, administrations, recherche.

F – Passerelles vers les autres spécialités

Certaines spécialités en Informatique et en Mathématiques appliquées.

G – Indicateurs de suivi du projet

Le suivi des enseignements se fera par le comité pédagogique de la formation composé des coordonnateurs de la formation, des enseignants intervenants et des délégués des étudiants (si nécessaires).

Ce comité se réunira trois fois par semestre au minimum et aura pour tâches

- de mettre au point des méthodes pédagogiques adéquates avec les objectifs visés,
- d'évaluer les enseignements et la formation (état d'avancement et autres),
- de mettre en place le parrainage des étudiants,
- de veiller à la cohérence du parcours et des stages,
- de faire le suivi des séminaires et des mémoires,
- d'évaluer le travail des étudiants.

Les PV des réunions seront transmis régulièrement aux :

- Chef de département d'informatique.
- Président du comité scientifique du département,
- Chefs des laboratoires impliqués,
- Vice doyen chargé de la pédagogie de la faculté des sciences de l'ingénieur.

5 – Moyens humains disponibles

A : Capacité d'encadrement

20 postes

(précisément 13 étudiants informaticiens et 7 étudiants mathématiciens)

B : Equipe d'encadrement de la formation

B-1 : Encadrement Interne

Nom, prénom	Diplôme	Grade	Laboratoire de recherche de rattachement	Type d'intervention *	Emargement
Noui Lemnouar	**Doctorat d'Etat**	**Prof.**	**Laboratoire des Techniques Mathématiques en Vue d'application : Aspects déterministes et stochastiques Université de Batna**	**Cours, TD, Encadrement de mémoires**	
Melekmi lamine	**Doctorat d'Etat**	**Prof**	**Département d'informatique**	**Cours, TD, Encadrement de mémoires**	
Benyousef Moussa	**Doctorat d'Etat**	**Prof**	**Département d'électronique**	**Cours, TD Encadrement de mémoire**	
Abdessemed Fodil	**Doctorat d'Etat**	**Prof**	**Département d'électronique**	**Cours, TD Encadrement de mémoire**	
Seghir Rachid	**Doctorat**	**M.C. classe B**	**Département d'informatique**	**Cours, TD,TP , Encadrement de mémoires**	

Behloul Ali	**Doctorat**	**M.C. classe B**	**Département d'informatique**	**Cours, TD, TP, Encadrement de mémoires**	
Hamouid Khaled	**Magister**	**M.A. classe A**	**Lastic**	**Cours, TD, Encadrement de mémoire**	
Toumi Mohamed	**Magister**	**M.A. classe A**	**Département d'informatique**	**Cours, TD, TP, Encadrement de mémoires**	
Nezzar Abderrafik	**Magister**	**M.A. classe A**	//	**Cours, TD, TP, Encadrement de mémoires**	
Nacer- Eddine BENABBAS	**Magister**	**M.A. classe A**	//	**Cours, TD, TP, Encadrement de mémoires**	
Betta Mohamed	**Magister**	**M.A. classe A**	//	**Cours, TD, TP, Encadrement de mémoires**	
Guitoune Abdelhafid	**Ingéniorat Inscrit en Magister**	**Assistant**	//	**Cours, TD,TP et Encadrement de mémoires**	
Dekhinet Abdalhamid	**Magister**	**M.A. classe A**	//	**Cours, TD, Encadrement de mémoire**	

- **= Cours, TD, TP, Encadrement de stage, Encadrement de mémoire.**

B-2 : Encadrement Interne

B-3 : Synthèse globale des ressources humaines

Grade	Effectif Interne	Effectif Externe	Total
Professeurs	04	00	
Maîtres de Conférences (A)	00	00	
Maîtres de Conférences (B)	03	00	
Maître Assistant (A)	07	00	
Maître Assistant (B)	00	00	
Autre (préciser) **Assistant**	01		
Total	**15**	**00**	

B-4 : Personnel permanent de soutien

Grade	Effectif
Ingénieur Informaticien	
Technicien supérieure en Informatique	

6 – Moyens matériels disponibles

A- Laboratoires Pédagogiques et Equipements : Fiche des équipements pédagogiques existants pour les TP de la formation envisagée (1 fiche par laboratoire)

Intitulé du laboratoire :

Capacité en étudiants : 20

N°	Intitulé de l'équipement	Nombre	Observations
01	Data Général machine Bi processeur 30 postes – Opérant sous Unix	01	
02	Centre de calcul équipe de 15 PC	03	
03	Imprimante réseaux	01	
04	Cluster de 8 PC – connexion à EumedGrid en projet	01	
05	Point d'accès internet Wireless	02	
06	Serveur Dell Bi-Processeurs	02	
07	Bibliothèque spécialisée –200 Ouvrages	01	
08	Amphithéâtres	03	
09	Salle de conférences pour séminaires	01	
10	Salles de TD	29	

B- Terrains de stage et formation en entreprise

Lieu du stage	Nombre d'étudiants	Durée du stage

C- Laboratoire(s) de recherche de soutien à la formation proposée

D- Projet(s) de recherche de soutien à la formation proposée :

Intitulé du projet de recherche	Code du projet	Date du début du projet	Date de fin du projet
L'algèbre et la transmission des données	B01320090029	01/01/2010	31/12/2012

E- Documentation disponible

1. Danny Poo, Derek Kiong et Swarnalatha Ashok. Object-Oriented Programming and JAVA. Second edition, Spring Verlag, 2008.
2. James Gosling, Bill Joy, Guy Steele et Gilard Bracha. The Java Language Specification. Third Edition. Addition-Wesley. 2005.
3. Stephen G. Kochan. Programming in C. Hayden Book Company, 1983.
4. David . A. Gustafon. Theory and Problems of Software Engineering. Schaum's outline Series. McGRAW-HILL.2002 .
5. Heinz Zukkighoven. Object-Oriented Construction Handbook. Elsevier and dpunkt.verlag.2005.
6. Stephen Gilbert et Bill Mc Carty. Object-Oriented Design in JAVA. 1998.
7. Rudolf Lid land Harald Niederreiter, Finite fields, Encyclopedia of Mathematics and applications, Cambridge university press, 1997.
8. M. Demazure. Cours d'algèbre. Primalité, divisibilité, codes. Cassini, 1997.
9. H.Kutner, C. Nachtsheim, J. Neter and W. Li, *Applied Linear Model*, 5 Edition, Mc Graw Hill, 2005.
10. Sureté de fonctionnement des systèmes informatiques, Jean- Claude Geffroy, Gilles Motet, Inter Editions. 1998.
11. Spécification et conception des systèmes, une méthodologie, J .P. Calver, Masson Editeur. 1992.
12, Transmissions et réseaux, Cours et exercices corrigés. Stéphane Lohier, Dunod
13, Internetworking with TCP/IP, 4th edition, de Douglas COMER
14. Computer Networks, 4th edition, de Andrew S. TANENBAUM
15. High Speed Networks and Internets, 2nd edition, de William STALLINGS
16. Abedjalil Ouahabi , Traitement du signal, Theorie du signal, Signaux deterministes ,OPU 87.
17. J.H. van Lint, *Introduction to coding theory*, 3eme edition, Springer
18. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press 2003
19. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, London, New York, Washington D.C., 2004.
20 - Dalhoumi S. « Cours de méthodologie », support de cours, Formation de formateurs, Cerist, Alger, Février 2004.
21. - Labasse B., « La communication scientifique ; principes et méthodes », Pôle Universitaire de Lyon, 2001
22- Mucchielli A., « La nouvelle communication : épistémologie des sciences de l'information – communication », Armand Collin, 2000
23. P. Fortin & R. Pomès, *Premiers pas en Maple,* Vuibert, 1995.
24. A. Leroux & R. Pomès, *Toutes les applications de Maple*, Vuibert, 1995.

25. Calcul formel, Mode d'emploi, exemples en Maple,
Philippe Dumas, Claude Gomez, Bruno Salvy, Paul Zimmermann, Masson. 1995
26. Aho & Hopcroft & Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, 1994.

27. Bini & Pan, *Polynomial and matrix computations*, Birkhäuser, 1994. 28. Cox & Little & O'Shea, *Ideal, varieties and algorithms*, Springer.

29. von zur Gathen et Gerhard, *Modern Computer Algebra*, 2nd edition, Cambridge University Press, 2003

30. B. Martin - "Codage, cryptologie et applications" - (éd. Presses Polytechniques et Universitaires Romandes (PPUR), 2004) - 354 p. - ISBN 978-2-88074-569-1
31. J.-G. Dumas, J.-L. Roch, E. Tannier et S. Varrette - "Théorie des codes (Compression, cryptage, correction)" - (éd Dunod, 2007) - 352 p. - ISBN 978-2-10-050692-7
32. R. E. Blahut, *Theory and Practice of Data Transmission Codes*. New York: Wiley, 1994.
33. S. B. Wicker, *Error-Control Systems for Digital Communication and Storage.* Englewood Cliffs, NJ: Prentice-Hall, 1995.
34. R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston: Kluwer Academic
Publishers, 1987. (A good reference for the algebra of finite fields.)
35. E. Berlekamp, ed., *Key Papers in the Development of Coding Theory*. New York: IEEE Press, 1974.
36. Berners-Lee, T., R. Fielding and H. Nielsen, 'Hypertext Transfer Protocol – HTTP/ 1.0', RFC 1945, May 1996.
37. Blakley, B., 'Architecture for Public-Key Infrastructure', Internet Draft, November 1996.
38. Boeyen, S., R. Housley, T. Howes, M. Myers and P. Richard, 'Internet Public Key Infrastructure Part 2: Operational Protocols', Internet Draft, March 1997.
39. F. Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977. Jürgen Bierbrauer

F- Espaces de travaux personnels et TIC :

- Bibliothèque de la Faculté des Sciences de l'ingénieur,
- Bibliothèque de la Faculté des Sciences.
- Bibliothèque du Laboratoire de recherche,
- Bibliothèque Centrale de l'Université,
- Connexion Internet.

II – Fiche d'organisation semestrielle des enseignements

1- Semestre 1

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales									
UEF1									
Eléments d'algèbre	63h	1h30	3h			8	8	x	X
UEF2									
Traitement de signal	63h	1h30	1h30	1h30		7	7	x	X
UE méthodologie									
UEM1									
Introduction à la programmation orientée objet	63h	1h30	1h30	1h30		5	5	x	X
Calcul formel	63h	1h30	1h30	1h30		6	6	x	X
UE Découverte									
UED1									
Ethique académique	21h	1h30				2	2	x	X
Anglais 1	21h	1h30				2	2	x	X
Total Semestre 1	294h	9h	7h30	4h30		30	**30**		

2- Semestre 2

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales									
UEF1									
Théorie des codes linéaires	63h	1h30	3h			7	7	x	X
UEF2									
Complexité algorithmique	42h	1h30	1h30			6	6	x	X
UEF3									
Réseaux	63h	1h30	1h30	1h30		7	7	x	X
UE méthodologie									
UEM									
Programmation orientée objet avancée	63h	1h30	1h30	1h30		5	5	x	X
Introduction à la cryptographie	42h	1h30		1h30		3	3	x	X
UE Découverte									
UED									
Anglais 2	21h	1h30				2	2	x	X
Total Semestre 2	294h	9h	7h30	4h30		30	**30**		

3- Semestre 3

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales									
UEF1									
Cryptographie avancée	63h	1h30	1h 30	1h30		8	8	x	x
UEF2									
Sécurité des réseaux	63h	1h30	1h30	1h30		6	6	x	x
UEF3									
Sûreté de fonctionnement des systèmes informatiques	42h	1h30	1h30			5	5	x	x
UE méthodologie									
UEM									
EDI et commerce électronique	42h	1h30		1h30		4	4	x	x
Recherche d'images par contenu	42h	1h30		1h30		3	3	x	x
UE Découverte									
UED									
Méthodologie de recherche	21h	1h30				2	2	x	x
Anglais 3	21h	1h 30				2	2	x	x
Total Semestre 3	294h	10h30	4h30	6h		30	**30**		

4- Semestre 4

Domaine : Mathématiques et informatique
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Mémoire sanctionné par une soutenance.

	VHS	Coeff	Crédits
Travail Personnel (mémoire)	280h00	22	22
Stage en entreprise			
Séminaires	21h00	8	8
Autre (préciser)			
Total Semestre 4	301	30	30

5- Récapitulatif global de la formation

VH \ UE	UEF	UEM	UED	UET	Total
Cours	168h00	126h00	105h		399h00
TD	210h00	63h			273h00
TP	84h00	126h00			210h00
Travail personnel	210h00	84h00	84h00		378h00
Autre (préciser)					
Total	672h00	399h00	189h		1260h00
Crédits	54	26	10		**90**
% en crédits pour chaque UE	60%	29%	11%		100%

III – Fiches d'organisation des unités d'enseignement

Libellé de l'UE : UEF1
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 1

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h00 **TD :** 42h00 **TP:** **Travail personnel :** 42h00
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF1 **Crédits :** 8 **Matière :** Eléments d'algèbre **Crédits :** 8 **Coefficient** : 8
Mode d'évaluation	Continu et examen
Description des matières	L'objectif de la première partie est d'introduire les notions fondamentales de la théorie des groupes. La deuxième permettra à l'étudiant d'acquérir les connaissances élémentaires sur les corps en particulier les corps finis, ces notions sont utiles dans l'études des codes linéaires

Libellé de l'UE : UEF2
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 1

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h **TD :** 21h **TP:** 21h **Travail personnel :** 21h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF2 **Crédits :** 7 **Matière :** Traitement de signal **Crédits**:7 **Coefficient :** 7
Mode d'évaluation	Continu et examen
Description des matières	Cette matière permet aux étudiants d'acquérir les connaissances et les outils du traitement du signal, ces notions sont utilisées pour accélérer certains algorithmes, en particulier les transformations de Fourrier sont indispensables pour le décodage de certains codes.

Libellé de l'UE : UEM
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Semestre : 1

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 42h **TD :** 42h **TP:** 42h **Travail personnel :** 21h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEM **Crédits :** 11 **Matière 1 :** Introduction à la programmation orientée objet **Crédits :** 5 **Coefficient :** 5 **Matière 2 :** Calcul formel **Crédits :** 6 **Coefficient :** 6
Mode d'évaluation	Continu et examen
Description des matières	**Matière 1** Ce module consiste en premier à rappeler les principes de la programmation impérative et le langage C avant d'introduire la programmation orientée objet. Ce rappel permettra de bien montrer l'apport de la programmation orientée objet dans le développement de logiciels. **Matière 2** L'objectif de ce cours est de donner une introduction aux principaux éléments du calcul formel et d'utiliser le logiciel Maple pour résoudre des problèmes analytiques, géométriques et algébriques. Le cours est accompagné d'un projet personnel.

Libellé de l'UE : UED
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Semestre : 1

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h **TD** : **TP:** Travail personnel : 21h
Crédits et coefficients affectés à l'UE et à ses matières	UE : UED 4 crédits **Matière 1** : Ethique académique Crédits : 2 Coefficient : 2 **Matière 2** : Anglais 1 Crédits : 2 Coefficient : 2
Mode d'évaluation (continu ou examen)	Continu et examen
Description des matières	**- Matière 1** Dispenser dans le cadre de ce cours les principes qui régissent le comportement des différents acteurs de l'enseignement supérieurs **- Matière 2** Ce module pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise.

Libellé de l'UE : UEF1
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 2

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h **TD :** 42h **TP:** **Travail personnel :** 42h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF1 **Crédits :** 7 **Matière :** Théorie des codes linéaires **Crédits :** 7 **Coefficient :** 7
Mode d'évaluation	Continu et examen
Description des matières	Le premier objectif est d'apprendre les méthodes du calcul modulaire, notions utiles pour la réalisation de certains cryptosystèmes. Le deuxième objectif de ce cours est de familiariser l'étudiant avec les notions fondamentales des codes correcteurs d'erreurs, cette étude utilise les notions élémentaires d'algèbre linéaire. Cette matière a des applications en théorie de l'information et en cryptographie.

Libellé de l'UE : UEF2
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 2

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h **TD :** 21h **TP :** **Travail personnel :** 21h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF2 **Crédits :** 6 **Matière :** Complexité algorithmique **Crédits :** 6 **Coefficient :** 6
Mode d'évaluation	Continu et examen
Description des matières	Introduire les notions de base en complexité. Cette notion intervient dans l'analyse des algorithmes.

Libellé de l'UE : UEF3
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 2

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h **TD :** 21h **TP:** 21h **Travail personnel :** 21h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF3 **Crédits :** 7 **Matière :** Réseaux **Crédits :** 7 **Coefficient :** 7
Mode d'évaluation	Continu et examen
Description des matières	L'objectif de ce cours est de donner aux étudiants de Master, des connaissances de base sur les réseaux. Ce cours présente les réseaux en général, puis passe à l'étude de TCP/IP avec quelques uns de ses mécanismes.

Libellé de l'UE : UEM
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 2

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 42h00 **TD :** 21h00 **TP:** 42h00 **Travail personnel :** 21h00
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEM **Crédits :** 8 **Matière 1 :** Programmation orientée objet avancée **Crédits :** 5 **Coefficient :** 5 **Matière 2 :** Introduction à la cryptographie **Crédits :** 3 **Coefficient :** 3
Mode d'évaluation	Continu et examen
Description des matières	**Matière 1** Dans ce module, on se concentre sur l'usage de la bibliothèque cryptographie, modèle de sécurité du langage JAVA. Le module sera illustré par un projet en petits groupes pour développer une application distribuée sécurisée. **Matière 2** Introduire les notions élémentaires de la cryptographie, étudier et analyser les cryptosystèmes classiques

Libellé de l'UE : UED
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Semestre : 2

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h **TD :** **TP :** Travail personnel : 21h
Crédits et coefficients affectés à l'UE et à ses matières	UE : UED 2 crédits **Matière** : Anglais 2 Crédits : 2 Coefficient : 2
Mode d'évaluation (continu ou examen)	Continu et examen
Description des matières	Ce module a pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise.

Libellé de l'UE : UEF1
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 3

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h00 **TD :** 21h00 **TP:** 21h 00 **Travail personnel :** 42h00
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF1 **Crédits :** 8 **Matière :** Cryptographie avancée **Crédits :** 8 **Coefficient :** 8
Mode d'évaluation	Continu et examen
Description des matières	Initier l'étudiant à l'étude des cryptosystèmes bases sur des problèmes algébriques ou des problèmes des codes correcteurs d'erreurs

Libellé de l'UE : UEF2
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 3

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h 00 **TD :** 21h00 **TP:** 21h00 **Travail personnel :** 21h00
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF2 **Crédits :** 6 **Matière:** Sécurité des réseaux **Crédits :** 6 **Coefficient** : 6
Mode d'évaluation	Continu et examen
Description des matières	Ce module a pour objectif d'initier les étudiants aux protocoles de sécurité dans les réseaux, et de se familiariser avec la taxonomie des failles de ces protocoles ainsi leur vérification via des logiques formelles

Libellé de l'UE : UEF3
Filière : Informatique
Spécialité : Cryptographie et Sécurité
Semestre : 3

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 21h00 **TD :** 21h00 **TP:** **Travail personnel :** 21h00
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEF3 **Crédits :** 5 **Matière :** Sûreté de fonctionnement des systèmes informatiques **Crédits :** 5 **Coefficient :** 5
Mode d'évaluation	Continu et examen
Description des matières	Maîtriser les bases théoriques de la sureté de fonctionnement des systèmes informatiques indépendamment du matériel employé, mettre en pratique les techniques d'évitement, de suppression et de tolérances aux fautes.

Libellé de l'UE : UEM
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Semestre : 3

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 42h **TD :** **TP:** 42h **Travail personnel :** 42h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UEM **Crédits :** 7 **Matière 1 :** EDI et commerce électronique Crédits : 4 Coefficient : 4 **Matière 2 :** Recherche d'images par contenu Crédits : 3 Coefficient : 3
Mode d'évaluation	Continu et examen
Description des matières	**Matière 1** Ce module a comme objectifs : • La réalisation d'une une étude complète sur le commerce électronique dans un contexte B2B (échanges d'entreprise à entreprise) ou B2C (échanges d'entreprises à consommateurs). • La sécurité dans le commerce électronique. **Matière 2** Ce cours fera une introduction sur les principes fondamentaux de la recherche d'images. Dans ce contexte, comment préserver la confidentialité et l'intégrité des informations cas particulier les images contre les utilisations frauduleuses.

Libellé de l'UE : UED
Filière : Informatique
Spécialité : Cryptographie et Sécurité

Semestre : 3

Répartition du volume horaire global de l'UE et de ses matières	**Cours :** 42h **TD :** **TP:** **Travail personnel :** 42h
Crédits et coefficients affectés à l'UE et à ses matières	**UE :** UED **Crédits :** 4 **Matière 2 :** Méthodologie de recherche **Crédits :** 2 **Coefficient :** 2 **Matière 2 :** Anglais 3 **Crédits :** 2 **Coefficient :** 2
Mode d'évaluation	Continu et examen
Description des matières	**Matière 1** Le but de ce cours est d'initier l'étudiant à la recherche scientifique en lui facilitant la tâche de la recherche bibliographique et la préparation de son mémoire de fin d'études en respectant les conventions et normes internationales. **Matière 2** Ce module a pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise.

IV - Programme détaillé par matière

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Eléments d'algèbre
Semestre : 1
Enseignant responsable de l'UEF1 : Mr. Noui Lemnouar
Enseignant responsable de la matière: . Noui Lemnouar

Objectifs de l'enseignement

La première partie introduit les notions fondamentales pour la théorie des groupes, des notions utiles pour la compréhension des corps et les codes linéaires ainsi que leurs applications.
La deuxième partie devrait permettre à l'étudiant d'acquérir les connaissances élémentaires que procure la théorie des corps finis.

Connaissances préalables recommandées

Algèbre 1 et Algèbre 2

Contenu de la matière :

Partie 1

1. Groupes, exemples
2. Homomorphismes
3. sous groupes, sous groupes distingues et groupes quotients.
4. Groupes cycliques, ordre des éléments, indice d'un sous groupe,
5. centre, centralisateur, sous groupe dérive, conjugaison,.
6. groupes particuliers.
7. Groupes de permutations.
8. Groupes de matrices

Partie 2

1. Définitions, caractéristiques, cardinal d'un corps fini,
2. Relation de frobenuis, morphisme de Frobenuis,
3. Construction et unicité des corps finis, construction pratique de Fq,
4. Sous corps d'un corps fini. élément primitif,
5. polynomes irréductibles et éléments conjugues,
6. Factorisation de x^n -1,
7. Congruences et Classes résiduelles.
8. Fonction Phi d'Euler.
9. Les Théorèmes de Fermat, Euler et de Lagrange
10. Transformée de Fourrier discrete.

Références

1. J. Querre, Cours d'algèbre, Maitrise de Mathématiques, Masson. 1976.
2. J. Calais. Éléments de théorie des groupes. PUF, 1998.
3. E. Ramis, C. Deschamps, et J. Odoux. Cours de Mathématiques 1, Algèbre. Dunod, 1998.
4 D.J.S. Robinson, "A course in the Theory of Groups," 2nd ed., Springer-Verlag, New York, 1995.

5. Rudolf Lid land Harald Niederreiter, Finite fields, Encyclopedia of Mathematics and applications, Cambridge university press, 1997.
6. M. Demazure. Cours d'algèbre. Primalité, divisibilité, codes. Cassini, 1997.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Traitement de signal

Semestre *:* 1

Enseignant responsable de l'UEF2 : Mr Benyoucef Moussa

Enseignant responsable de la matière: Mr Benyoucef Moussa, Dekhinet

Objectifs de l'enseignement

Cette UE permet aux étudiants d'acquérir les connaissances et les outils du traitement du signal, Ces notions sont utilisées pour accélérer certains algorithmes, en particulier les transformations de Fourrier sont indispensables pour le décodage de certains codes.

Connaissances préalables recommandées

Outils mathématiques de la première année,

Contenu de la matière

1. **Généralités sur les signaux,**
   Signal- définition
   Notation des signaux
   Classification des signaux
   Caractérisation des signaux (énergie, puissance d'un signal…)
   Exemples de quelques signaux particuliers (Dirac, Echelon, sinc,,,,,)
2. **Théorie de l'information**
   Mesure de la quantité d'information,
   Entropie, codage de l'information,
   Capacité du canal d'information.
3. **Présentation vectorielle des signaux**
   Notion d'espace vectoriel (norme, distance, espace de Hilbert)
   Produit scalaire et orthogonalité des signaux.
   Approximation des signaux,
4. **Analyse de Fourier**.
   Base de Fourier
   Séries de Fourrier, Transformation de Fourier
   Notion de spectre.
5. **Echantillonnage**
   Principe d'échantillonnage.
   Types d'échantillonnage (théorème de Shanon)
   Relations entre le spectre du signal et le spectre échantillonnée.
   Quantification.
   Notion de corrélation, de convolution.
   Transformée en Z.
   Transformée de Fourier discrète.
   Transformée de Fourier rapide.

Références

1) Abedjalil Ouahabi , Traitement du signal, Théorie du signal, Signaux déterministes ,OPU 1987.
2) Christiane Rousseau, Yvan Saint-Aubin , Mathématiques et Technologie, 2008 Springer Science+ Business Media, LLC.
3) François Liret**,** MATHS EN PRATIQUE à l'usage des étudiants **,** Cours et exercices Dunod 2006.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Introduction à la programmation Orientée Objet

Semestre *:* 1

Enseignant responsable de l'UEM : Mr Betta Mohamed

Enseignant responsable de la matière: Mr Betta Mohamed

Objectifs de l'enseignement

Ce module consiste en premier à rappeler les principes de la programmation impérative et le langage C avant d'introduire la programmation orientée objet. Ce rappel permettra de bien montrer l'apport de la programmation orientée objet dans le développement de logiciels , et l'étude du langage de programmation JAVA largement utilisé dans l'industrie informatique, plus particulièrement dans les applications WEB.

Connaissances préalables recommandées

Algorithme et structures de données

Contenu de la matière

1- Rappel sur la programmation impérative
2- Langage C
3- Programmation Orientée Objet
    a. Motivations
    b. Notion d'objet
    c. Notion de classe
    d. Relation entre classe et objet
    e. Notion d'encapsulation
    f. Héritage et polymorphisme
4- Langage JAVA
    a. Objet
    b. Classe
    c. Héritage
    d. Swing
    e. Applets
    f. Servlets
    g. RMC et Threads

Références:

[1] Danny Poo, Derek Kiong et Swarnalatha Ashok. Object-Oriented Programming and JAVA. Second edition, Spring Verlag, 2008.

[2] James Gosling, Bill Joy, Guy Steele et Gilard Bracha. The Java Language Specification. Third Edition. Addition-Wesley. 2005.

[3] Stephen G. Kochan. Programming in C. Hayden Book Company, 1983.

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Calcul Formel
Semestre *:* 1
Enseignant responsable de l'UEM: Mr Betta Mohamed
Enseignant responsable de la matière: Mr Toumi Mohamed et Melekmi Lamine.

Objectifs de l'enseignement

L'objectif de ce cours est de donner une introduction aux principaux éléments du calcul formel et d'utiliser le logiciel Maple pour résoudre des problèmes géométriques et algébriques. Le cours est accompagné d'un projet personnel.

Connaissances préalables recommandées

Connaissances en analyse, algèbre linéaire et géométrie du niveau Licence.

Contenu de la matière

1. Présentation des logiciels

1.1. Calcul formel versus calcul numérique.
1.2. Présentation générale de logiciels différents de calcul formel (Maple, Mathématica,).

2. Notions de base de calcul formel en Maple

2.1. Données et opérateurs
2.2. Symboles et variables
2.3. Expressions, évaluations et simplifications
2.4. Fonctions et procédures
2.5. Structures et opérations itératives
2.6. Conditionnement, programmation. Packages.

3. Domaines d'utilisation et applications

3.1. **Arithmétique**
3.1.1. Calculs entiers et rationnels
3.1.2. Divisibilité et primalité
3.1.3. Fractions continues
3.1.4. _Equations en nombres entiers
3.1.5 Applications de l'algorithme de Euclide.
3.2. **Calcul matriciel**
3.2.1. Matrices et vecteurs
3.2.2. Les objets vecteurs et matrice en Maple
3.2.3 Manipulation des matrices
3.2.4. Calculs matriciels de base
3.2.5. Résolution de systèmes linéaires
3.2.6. Calculs sur des matrices
3.2.7 Optimisation linéaire
3.2.8 Automatique

3.3. **Espaces vectoriels euclidiens**
3.3.1. Isométries
3.3.2. Réduction d'une forme quadratique
3.3.3. Optimisation quadratique
3.4 **Polynômes et fractions rationnelles**
3.4.1. Opérations purement syntaxiques
3.4,2 Récriture et simplification
3.4.3. Calculs en une variable
3.5. **Polynômes et systèmes multivariés**
3.5.1. Bases de Grobner
3.5.2. Applications
3.6. **Suites réelles**
3.6.1. Récurrences linéaires
3.6.2 Coeffi_cients constants
3.6.3 Coeff_cients polynomiaux
3.6.4 Récurrences d'ordre un
3.6.5 Récurrences du type un+1 = f(un)
3.6.6 Récurrences du type un+1 = f(n; un)

4. Projet personnel

Projet personnel pour la résolution d'un problème en algèbre, équations différentielles, géométrie différentielle.

Références

1. P. Fortin & R. Pomès, *Premiers pas en Maple,* Vuibert, 1995.

2. A. Leroux & R. Pomès, *Toutes les applications de Maple*, Vuibert, 1995.

3. Calcul formel, Mode d'emploi, exemples en Maple,
Philippe Dumas, Claude Gomez, Bruno Salvy, Paul Zimmermann Masson. 1995

4. Aho & Hopcroft & Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, 1994.

5. Bini & Pan, *Polynomial and matrix computations*, Birkhäuser, 1994.

6. Cox & Little & O'Shea, *Ideal, varieties and algorithms*, Springer.

7. von zur Gathen et Gerhard, *Modern Computer Algebra*, 2nd edition, Cambridge University Press, 2003

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Ethique académique
Semestre *:* 1

Enseignant responsable de l'UED : Mr **Nacer- Eddine BENABBAS**
Enseignant responsable de la matière: Mr **Nacer- Eddine BENABBAS**

Objectifs de l'enseignement

Dispenser dans le cadre de ce cours les principes qui régissent le comportement des différents acteurs de l'enseignement supérieurs. Un accent particulier sera mis sur l'éthique en matière de publication de papiers scientifique.

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

Introduction
Science et éthique
Ethique dans l'enseignement supérieur
Ethique dans la publication de papiers de recherche

Références

- *IEEE ethics in paper publishing , www.IEEE.org*

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Anglais **1**
Semestre *:* 1

Enseignant responsable de l'UED : Mr Nacer- Eddine BENABBAS
Enseignant responsable de la matière: Mr Nacer- Eddine BENABBAS

Objectifs de l'enseignement

Ce module a donc pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

1. *La première partie concerne un travail sur des documents récents lui permettent d'être au courant des dernières innovations du domaine de la haute technologie.*

2. *La deuxième partie du cours est consacrée aux documents déjà présenté. Ceci permet à l'étudiant de parfaire sa production orale. Des revues de presse hebdomadaires sont également présentées.*

Références *(Livres et polycopiés, sites internet, etc).*

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Théorie des codes linéaires
Semestre *:* 2
Enseignant responsable de l'UEF1 : Mr. Noui Lemnouar
Enseignant responsable de la matière: Mr. Noui lemnouar

Objectifs de l'enseignement

L'objectif de ce cours est de familiariser l'étudiant avec les notions fondamentales des codes correcteurs d'erreurs, cette étude utilise les notions élémentaires d'algèbre linéaire. Cette matière a des applications en théorie de l'information et en cryptographie.

Connaissances préalables recommandées

Algèbre 1 et Algèbre 2.

Contenu de la matière

I) Rappel sur l'arithmétique

1. Congruences et Classes résiduelles, fonction Phi d'Euler.
2. Les Théorèmes de Fermat, Euler et de Lagrange
3. Résidualités quadratiques

II) Codes Linéaires

1.Introduction des codes linéaires.
2 Codes correcteurs d'erreurs.
3 Description par des matrices génératrices
4 Description par des matrices de contrˆole
5 Décodage d'un code linéaire, par le tableau standard, par le syndrome.
6. Codes duaux, codes auto-duaux.
7. Equivalence des codes, groupes d'automorphismes.

III). Exemples de codes linéaires

A) Codes de Hamming, décodage.
B) Codes de Hamming étendus
C) Codes de Reed Muller.
D) Codes cycliques
E) Codes BCH.
F) Codes de Goppa.

IV) Application des codes linéaires dans l'industrie

a) Code du disque compact.
b) Code des CD-Rom…..

Références

[1] J.H. van Lint, *Introduction to coding theory*, 3eme edition, Springer
[2] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press 2003
[3]. F. Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977. Jürgen Bierbrauer.

[4]. *Introduction to Coding Theory*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, London, New York, Washington D.C., 2004.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Complexité algorithmique.

Semestre *:* 2

Enseignant responsable de l'UEF2 : Mr. Seghir Rachid

Enseignant responsable de la matière: Seghir rachid et Melekmi lamine

Objectifs de l'enseignement

L'objectif de ce module est de présenter les grands principes de la complexité algorithmique. Il s'agit de montrer les différentes classes de problèmes et la façon dont la complexité d'un algorithme est calculée afin d'analyser ses performances.

Connaissances préalables recommandées

Connaissances en programmation et en mathématiques du niveau Licence.

Contenu de la matière :

1. Introduction
2. Calcul de coût d'un algorithme
3. Complexité en temps et en espace
4. Machines de Turing
    a) Machines équivalentes.
    b) Machines de Turing non déterministes
    c) Machines de Turing universelles
5. Langage reconnu par une machine de Turing
6. Problème de décision.
7. Problèmes P, NP, NP-dur et autres.
    a) Le problème « Premier » est NP.
    b) Le problème de satisfaisabilité
    c) Le problème TSP
8. Algorithmes déterministes
9. Algorithmes probabilistes
10. Réduction et complétude
11. Théorie de la complexité et la cryptographie moderne.

Références

1) T. Cormen, C. Leiserson, R. Rivest. Introduction à l'algorithmique. Dunod, 1994
2) I. Lavallée, Complexité et algorithmique avancée - Une introduction. Hermann, 2008.
3) Christos H. Papadimitriou. Coputational complexity. Addison-Wesely. 1994
4) S. Arora, B. Barak. Computational complexity: A modern approach. Cambridge 2007
5) Douglas Stinson, *Cryptographie - Théorie et Pratique* (Vuibert, 2003)
6) Gilles Zemor : *Cours de Cryptographie* (Cassini, 2000)
7) Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997)
8) Neal Koblitz, *A Course in Number Theory and Cryptography* (GTM 114, Springer, 1994)

9) Henri Cohen, *A course in computational algebraic number theory* (4 édition, GTM 138, Springer-Verlag, 2000)
10) Henri Cohen, *Advanced topics in computational number theory* (GTM 193, Springer-Verlag, 2000

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Réseaux

Semestre *:* 2

Enseignant responsable de l'UEF3 : Mr. Toumi Mohamed

Enseignant responsable de la matière: Toumi Mohamed

Objectifs de l'enseignement

L'objectif de ce cours est de donner aux étudiants de Master, des connaissances de base sur les réseaux. Ce cours présente les réseaux en général, puis passe à l'étude de TCP/IP avec quelques uns de ses mécanismes.

Connaissances préalables recommandées

Connaissances de la première année Licence.

Contenu de la matière :

1ère partie Principe des réseaux.

1.1 Introduction
1.2 Le modèle de référence OSI de l'ISO
1.3 La couche physique : Transmission en bande de base, transmission modulée, multiplexage et les supports de transmission
1.4 La couche liaison : Détection et correction d'erreurs et les protocoles de liaison de données
1.5 La couche réseau
  1.5.1 Le contrôle de flux
  1.5.2 Le problème de la congestion
  1.5.3 Le routage
1.6 La couche transport
1.7 Les couches hautes : session, présentation et application

2ème Partie : Le réseau Internet et les protocoles TCP/IP.

2.1 Architecture des protocoles TCP/IP
2.2 Adressage
2.3 La couche liaison
2.4 Le protocole IP
2.4.1 Le datagramme IP
2.4.2 La fragmentation des datagrammes IP
2.4.3 Le routage IP
2.4.4 La gestion des erreurs
2.5 Les protocoles TCP et UDP
2.5.1 Le protocole UDP
2.5.2 Le protocole TCP
2.6 Les applications (FTP, TFTP, Telenet, SMTP, HTTP, DHCP…)
2.7 Quelques commandes utiles

Références

1) Transmissions et réseaux, Cours et exercices corrigés. Stéphane Lohier, Dunod
2) Internetworking with TCP/IP, 4th edition, de Douglas COMER
3) Computer Networks, 4th edition, de Andrew S. TANENBAUM
4) High Speed Networks and Internets, 2nd edition, de William STALLINGS

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Programmation orientée objet avancée.

Semestre *:* 2

Enseignant responsable de l'UEM : Betta Mohamed

Enseignant responsable de la matière: Betta Mohamed

Objectifs de l'enseignement

Dans ce module, on se concentre sur l'usage de la bibliothèque cryptographie, modèle de sécurité du langage JAVA. Le module sera illustré par un projet en petits groupes pour développer une application distribuée sécurisée.

Connaissances préalables recommandées

Programmation Orientée Objet et Génie Logiciel

Contenu de la matière

1. Modèles de développement de logiciel
    - Assemblage de composants
    - Modèle en spirale

2. Développement sécurisé
    - la définition d'une analyse de risque (identification des menaces, des hypothèses d'utilisation du produit, etc.) ;
    - les méthodes de mise en place de contre-mesures efficaces et exhaustives
    - les méthodes formelles ou semi-formelles (preuve de sécurité) ;
3. Langage Java et J2EE : utilisation de la bibliothèque Cryptographie de JAVA ; ainsi que le module de sécurité pour développer une application distribuée sécurisée.

Références:

[1] Danny Poo, Derek Kiong et Swarnalatha Ashok. Object-Oriented Programming and JAVA. Second edition, Spring Verlag, 2008.
[2] David . A. Gustafon. Theory and Problems of Software Engineering. Schaum's outline Series. McGRAW-HILL.2002 .
[3] James Gosling, Bill Joy, Guy Steele et Gilard Bracha. The Java Language Specification. Third Edition. Addition-Wesley. 2005.
[4] Heinz Zukkighoven. Object-Oriented Construction Handbook. Elsevier and dpunkt.verlag.2005.
[5] Stephen Gilbert et Bill Mc Carty. Object-Oriented Design in JAVA. 1998.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Introduction à la cryptographie.

Semestre *:* 2

Enseignant responsable de l'UEM : Betta Mohamed

Enseignant responsable de la matière: Seghir Rachid.

Objectifs de l'enseignement

Introduire les notions élémentaires de la cryptographie, étudier et analyser les cryptosystèmes classiques

Connaissances préalables recommandées

Module de l'algèbre 1 et l'algèbre 2, programmation

Contenu de la matière

1. Introduction
2. Aperçu historique.
3. Terminologie
4. Cryptographie invulnérable
5. Mécanismes de la cryptographie
6. Cryptographie conventionnelle
    a) Chiffrement par substitution
    b) Chiffrement par transposition
    c) Chiffrement de César
    d) Gestion des clés et cryptage conventionnel
7. Cryptographie de clé privée (symétrique)
    a) Exemples (DES, 3-DES, AES ; …)
8. Cryptographie de clé publique (asymétrique)
    a) Exemples (RSA ; Elgamel, …).
9. Protocoles de sécurité.
    a) Protocoles d'authentification
    b) Protocoles de distribution de clés
    c) Protocoles "zero knowledge"
10. Protocoles de commerce électronique

Références

1. Schneier Bruce, Cryptographie appliquée – Algorithmes, protocoles et code source en C. Tomson 1997.
2. Johannes A. Buchmann, Introduction to Cryptography, Springer 2000.
3. Menezes Alfred J., van Oorschot Paul C., Vanstone Scott A. Handbook of Applied Cryptographie. CRC Press LLC 1999.
4. Ireland & Rosen, *A Classical Introduction to Modern Number Theory*, Springer.
5. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994
6. Koblitz, *Algebraic Aspects of Cryptography*, Springer.
7. Schneier, *Cours de Cryptographie appliquée*, Wiley.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Anglais **2**
Semestre *:* 2

Enseignant responsable de l'UED : Mr Nacer- Eddine BENABBAS
Enseignant responsable de la matière: Mr Nacer- Eddine BENABBAS

Objectifs de l'enseignement

Ce module a donc pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

1. *La première partie concerne un travail sur des documents récents lui permettent d'être au courant des dernières innovations du domaine de la haute technologie.*

2. *La deuxième partie du cours est consacrée aux documents déjà présenté. Ceci permet à l'étudiant de parfaire sa production orale. Des revues de presse hebdomadaires sont également présentées.*

Références

Mode d'évaluation : Continu et examen.

Intitulé du Master **Cryptographie et Sécurité**
Intitulé de la matière Cryptographie avancée
Semestre *:* 3
Enseignant responsable de l'UEF1 : Mr Noui lemnouar
Enseignant responsable de la matière : Mr Noui Lemnouar

Objectifs de l'enseignement
Initier l'étudiant à l'étude des cryptosystèmes basés sur des problèmes algébriques ou des problèmes des codes correcteurs d'erreurs.
Connaissances préalables recommandées
Module de l'algèbre 1 et l'algèbre 2, module des corps finis, module des codes correcteurs d'erreurs.

Contenu de la matière
1. Introduction
- Besoins de sécurité
- Crypto-Systèmes Symétrique
- Crypto-Systèmes Asymétrique
- Fonctions de Hashage
- Signature Électronique
- Nouvelles Tendances en Cryptographie
- Cryptanalyse

2.Cryptosystemes.
- La méthode RSA
- La méthode du sac à dos.
- Fonction « one-way ».
- Logarithme discret et cryptosysteme d'El gamel
- Factorisation des entiers et cryptosystème de RSA.
- Codes correcteurs d'erreurs et cryptosystème de Mc Elièce.

3. Authentification
- Protocoles, Principes
- Techniques, signature et partage
- Signature numérique,
- Signature arbitrée.
- Signature à l'aide des clés publiques.
- Sécurité des fichiers.
- Algorithmes, exemples.

Références

1. Ireland & Rosen, *A Classical Introduction to Modern Number Theory*, Springer.
2. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994
3. Blake, Seroussi et Smart, *Elliptic Curves in Cryptography*, Springer.
4. Koblitz, *Algebraic Aspects of Cryptography*, Springer.

5. Schneier, *Cours de Cryptographie appliquée*, Wiley.
6. Gilles Zemor : *Cours de Cryptographie* (Cassini, 2000)

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Sécurité des réseaux
Semestre *:* 3
Enseignant responsable de l'UEF2 : Nezzar Abderrafik
Enseignant responsable de la matière: Nezzar Abderrafik et Hamouid

Objectifs de l'enseignement

L'objectif de ce cours est de donner aux étudiants de Master, des connaissances de base sur les réseaux. Ensuite initier les étudiants aux protocoles de sécurité dans les réseaux, et de se familiariser avec la taxonomie des failles de ces protocoles ainsi leur vérification via des logiques formelles

Connaissances préalables recommandées

Notions élémentaires d'informatiques.

Contenu de la matière

1) Introduction.
2) Protocoles de sécurité.
   - Protocoles d'authentification
   - Protocoles de distribution de clés
   - Protocoles "zero knowledge"
   - Protocoles de commerce électronique
3) Taxonomie des failles dans les protocoles de sécurité
   - Introduction
   - Trace d'exécution.
   - Failles des protocoles cryptographiques.
   - Failles de fraîcheur.
   - Failles d'oracle.
   - Failles d'association.
   - Failles d'implantation.
   - Failles de répudiation.
   - Conclusion
4) Spécifications et vérifications formelles des protocoles de sécurité :
   4-1) Logiques BAN
      - Syntaxe de BAN.
      - Postulats de la logique BAN.
      - Idéalisation de protocoles.
      - Analyse de protocoles.
      - Formalisation de la propriété d'authentification.
      - Exemples
   4-2) Calcul SPI
      - Syntaxe de SPI.
      - Sémantique de SPI
      - Vérification des protocoles cryptographiques.

Références .

1. Cryptography and Network Security: Principles and Practice, 3rd Edition William Stallings – Prentice Hall 2002
2. A Logic of Authentication, M. Burrows, M. Abadi, and R.Needham. ACM Transactions on Computer Systems (TOCS)Volume 8 , Issue n 1 (February 1990) Pages: 18 - 36 .
3. Transmissions et réseaux, Cours et exercices corrigés. Stéphane Lohier,Dunod
4. Internetworking with TCP/IP, 4th edition, de Douglas COMER
5. Computer Networks, 4th edition, de Andrew S. TANENBAUM
   High Speed Networks and Internets, 2nd edition, de William STALLINGS

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Sûreté de fonctionnement des systèmes informatiques

Semestre *:* 3

Enseignant responsable de l'UEF3: Guitoune Abdelhafid

Enseignant responsable de la matière: Guitoune Abdelhafid

Objectifs de l'enseignement

Maîtriser les bases théoriques de la sureté de fonctionnement des systèmes informatiques indépendamment du matériel employé, mettre en pratique les techniques d'évitement, de suppression et de tolérances aux fautes.

Connaissances préalables recommandées

Notions élémentaires d'informatiques.

Contenu de la matière

1, Problématique de la sureté de fonctionnement des systèmes informatiques
2. Mécanismes destructeurs.
3. Les défaillances et leurs causes
4. Définitions des fautes et de leurs effets
5. Modèles de fautes des technologies matérielles et logicielles.
6. Mécanismes protecteurs
7. Evaluation de la sûreté de fonctionnement
8. La redondance
9. Les codes détecteurs et correcteurs d'erreurs.
10. Panorama des méthodes de protection.
11. Test en ligne
12. Systèmes à défaillances non dangereuses.
13. Synthèse comparative.

Références

1. Sureté de fonctionnement des systèmes informatiques, Jean- Claude Geffroy, Gilles Motet, InterEditions. 1998.
2. Spécification et conception des systèmes, une méthodologie, J .P. Calver, Masson Editeur. 1992.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : EDI et commerce électronique

Semestre *:* 3

Enseignant responsable de l'UEM: Mr. Behloul Ali

Enseignant responsable de la matière: Betta Mohamed

Objectifs de l'enseignement

Ce module a comme objectifs :

- La réalisation d'une une étude complète sur le commerce électronique dans un contexte B2B (échanges d'entreprise à entreprise) ou B2C (échanges d'entreprises à consommateurs).
- La sécurité dans le commerce électronique.

Connaissances préalables recommandées

Notions élémentaires d'informatiques.

Contenu de la matière :

1. Principes du e-business
    a) Stratégies
    b) Business models
    c) Systèmes d'information étendus
2. Plates-formes e-business
    a) sites commerciaux
    b) Catalogues en ligne
    c) Plates-formes d'achat
    d) Places de marché électronique
    e) Portails spécialisés
3. Modélisation des processus et rôle des progiciels intégrés (ERP, CRM…) ;
4. Commerce électronique B2B
    a) Etat de l'art EDI
    b) Initiation UML/XML
    c) Web-EDI
5. Sécurité et paiement électronique.
6. Sécurité des agents mobiles
7. Sécurité du commerce mobile
8. Sécurité de la carte à puce

Références:

[1] Wil van der Aalst et Kees van Hee. Workflow Management : Models , Methods and Systems. The MIT Press Cambridge Massachusetts London, England. 2002.

[2] E-Business Innovation and Process Management. In Lee, Western Illinois University, USA, Cybertech Publishing 2007.

[3] Vesna Hassler. Security Fundamentals for E-Commerce. Artech House INC, 2001.

Mode d'évaluation : Continu et examen

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Recherche d'images par contenu

Semestre *:* 3

Enseignant responsable de l'UED : Mr. Behloul Ali

Enseignant responsable de la matière: Mr. Behloul Ali

Objectifs de l'enseignement

Ce cours fera une introduction sur les principes fondamentaux de la recherche d'images. Dans ce contexte, comment préserver la confidentialité et l'intégrité des informations cas particulier les images contre les utilisations frauduleuses.

Connaissances préalables recommandées

Programmation et génie logiciel

Contenu de la matière :

1. Problématique de la recherche d'image par le contenu.
    a) Globale
    b) Locale
2. Introduction au traitement numérique d'images
    a) Compression
    b) Tatouage,…
3. Reconnaissance de formes pour la sécurité
    a) Reconnaissance de visage
    b) Reconnaissance d'empreinte digitale
4. Critères d'évaluation d'un système de recherche par le contenu
    a) Précision-rappel
    b) F-Mesure

Bibliographie

1. Diagnostic et reconnaissance des formes, D.Bernard , Lavoisier 1990.
2. Traitement et analyse des images numériques, S.Bres J.Jolion F.Lebourgeois, Lavoisier 2003.
3. M. Milgram, Reconnaissance des formes, méthodes numériques et connexionnistes, édition (Armand Colin, 1993)
4. "Documentaliste Sciences de l'information". Vol. 42 - N° 6. Décembre 2005. La revue "Documentaliste".
5. S. Pal, P. Mitra, "Pattern Recognition Algorithms for Data Mining", edition Chapman and Hall (2004).

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Méthodologie de la recherche
Semestre *:* 3
Enseignant responsable de l'UEM : Mr. Seghir Rachid
Enseignant responsable de la matière: Mr. Seghir Rachid

Objectifs de l'enseignement

Permettre aux étudiants de s'initier aux principales méthodes de recherche, de mener correctement un projet de recherche, et de savoir communiquer les résultats de la recherche.

Connaissances préalables recommandées

Contenu de la matière :

- *La recherche publique et en entreprise*
- *Méthodes de recherche*
- *L'évaluation de la recherche*
- *Les outils d'un chercheur*
- *Communication des résultats de la recherche.*

Références

1. Dalhoumi S. « Cours de méthodologie », support de cours, Formation de formateurs, Cerist, Alger, Février 2004.
2. Labasse B., « La communication scientifique ; principes et méthodes », Pôle Universitaire de Lyon, 2001
3. Mucchielli A., « La nouvelle communication : épistémologie des sciences de l l'information – communication », Armand Collin, 2000
4. Salvador Juan. « Méthodes de recherche en sciences socio-humaines : Approche critique des techniques », Presses Universitaires de France (PUF), 1999, p304.

Mode d'évaluation : Continu et examen.

Intitulé du Master : Cryptographie et Sécurité

Intitulé de la matière : Anglais **3**
Semestre *:* 2

Enseignant responsable de l'UED : Mr Seghir Rachid
Enseignant responsable de la matière: Mr Nacer- Eddine BENABBAS

Objectifs de l'enseignement

Ce module a donc pour objectif de rendre l'étudiant d'avantage autonome dans son expression orale et écrite, ainsi que dans sa capacité à comprendre un document scientifique en langue anglaise

Connaissances préalables recommandées

Notions de la première année.

Contenu de la matière

3. *La première partie concerne un travail sur des documents récents lui permettent d'être au courant des dernières innovations du domaine de la haute technologie.*

4. *La deuxième partie du cours est consacrée aux documents déjà présenté. Ceci permet à l'étudiant de parfaire sa production orale. Des revues de presse hebdomadaires sont également présentées.*

Références

Mode d'évaluation : Continu et examen.

V- Accords ou conventions

LETTRE D'INTENTION TYPE

(En cas de master coparrainé par un autre établissement universitaire)

(Papier officiel à l'entête de l'établissement universitaire concerné)

Objet : Approbation du coparrainage du master intitulé :

Par la présente, l'université (ou le centre universitaire) déclare coparrainer le master ci-dessus mentionné durant toute la période d'habilitation de ce master.

A cet effet, l'université (ou le centre universitaire) assistera ce projet en :

- Donnant son point de vue dans l'élaboration et à la mise à jour des programmes d'enseignement,
- Participant à des séminaires organisés à cet effet,
- En participant aux jurys de soutenance,
- En œuvrant à la mutualisation des moyens humains et matériels.

SIGNATURE de la personne légalement autorisée :

FONCTION :

Date :

LETTRE D'INTENTION TYPE

(En cas de master en collaboration avec une entreprise du secteur utilisateur)

(Papier officiel à l'entête de l'entreprise)

OBJET : Approbation du projet de lancement d'une formation de master intitulé :

Dispensé à :

Par la présente, l'entreprise déclare sa volonté de manifester son accompagnement à cette formation en qualité d'utilisateur potentiel du produit.

A cet effet, nous confirmons notre adhésion à ce projet et notre rôle consistera à :

- Donner notre point de vue dans l'élaboration et à la mise à jour des programmes d'enseignement,
- Participer à des séminaires organisés à cet effet,
- Participer aux jurys de soutenance,
- Faciliter autant que possible l'accueil de stagiaires soit dans le cadre de mémoires de fin d'études, soit dans le cadre de projets tuteurés.

Les moyens nécessaires à l'exécution des tâches qui nous incombent pour la réalisation de ces objectifs seront mis en œuvre sur le plan matériel et humain.

Monsieur (ou Madame)…….est désigné(e) comme coordonateur externe de ce projet.

SIGNATURE de la personne légalement autorisée :

FONCTION :

Date :

CACHET OFFICIEL ou SCEAU DE L'ENTREPRISE

VI – Curriculum Vitae des Coordonnateurs